הגדרה: חוג הוא קבוצה R עם שתי פעולות בינאריות

$+ : R\times R \to R$

$\cdot : R\times R \to R$

כך ש- $(R,+)$ חבורה אבלית:

1) $a+(b+c)=(a+b)+c$ לכל $a,b,c\in R$

2) קיים איבר $0\in R$ כך ש $a+0=0+a=a$ לכל $a\in R$

3) לכל $a\in R$ קיים $-a\in R$ כך ש $a+(-a)=(-a)+a=0$

4) $a+b=b+a$ לכל $a,b\in R$

0 יחיד

בהינתן a, $-a$ יחיד

$(R,\cdot)$ הוא מונואיד:

5) $a(bc)=(ab)c$ לכל $a,b,c\in R$

6) קיים איבר $1\in R$ כך ש- $a\cdot 1=1\cdot a=a$ לכל $a\in R$

1 יחיד

חוק הפילוג:

7) $a(b+c)=ab+ac$ לכל $a,b,c\in R$

8) $(b+c)a=ba+ca$ לכל $a,b,c\in R$

הגדרה: נאמר $ab=ba$ לכל $a,b\in R$ ואומרים כי R חילופי/קומוטטיבי.

טענה:

יהי R חוג. לכל $a\in R$ מתקיים $0\cdot a=a\cdot 0=0$

הוכחה:

$$0=(0+0)$$

פילוג: $0\cdot a=(0+0)a=0\cdot a+0\cdot a$

נוסיף $-0\cdot a$ לשני האגפים $0=0\cdot a$

הגדרה: R נקרא חוג עם חילוק אם לכל $a\neq 0\in R$ קיים a^{-1} כך ש- $a\cdot a^{-1}=a^{-1}\cdot a=1$

הגדרה: R נקרא שדה אם R הוא חוג עם חילוק חילופי.

הערה:

כל חוג סופי עם חילוק הוא בהכרח חילופי, לכן שדה (נוכיח בהמשך)

דוגמאות:

1) $R=\mathbb{Z}$ עם חיבור וכפל רגילים

2) יהי $n\in\mathbb{N}$. $R=\mathbb{Z}_n$ עם חיבור וכפל מחלקות $[0]=0$ $[1]=1$

3) $R=\{0\}$ $0=0+0$, $0=0\cdot 0$ $(1=0)$ החוג הנ"ל נ.א.ג.

4) יהי R חוג כלשהו. חוג הפולינומים

$$R[x]=\{a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0 \mid a_i\in R,\ n\in\mathbb{N}_0\}$$

חיבור:

$$\sum_{i=0}^{n} a_ix^i+\sum_{i=0}^{n} b_ix^i=\sum_{i=0}^{n}(a_i+b_i)x^i$$

כפל:

$$(a_1x+a_0)(b_1x+b_0)=(a_1x)(b_1x)+(a_1x)b_0+a_0(b_1x)+a_0b_0=$$

$$=a_1b_1x^2+(a_1b_0+a_0b_1)x+a_0b_0$$

(x מתחלף בכלל עם כל הסקלארים $a\in R$)

5) R חוג. נקבל חוג של פולינומים ב- n משתנים, $n\in\mathbb{N}$

$$R[x_1,\dots,x_n]=\left\{\sum_{(i_1,\dots,i_n)=\bar{i}} a_{\bar{i}}\,x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \;\middle|\; \begin{array}{l} a_{\bar{i}}\neq 0 \\ a_{\bar{i}}\in R \end{array}\right\}$$

סופי, של $\bar{i}$-ים שבהם מספר

$$(n_1,\dots,n_n)\in\mathbb{N}_0^n$$

$$2x_1^{100}x_2^2+613x_1x_2^4\in\mathbb{Z}[x_1,x_2]$$

המשתנים $x_i x_j=x_j x_i$ מתחלפים כמו עם כל ואחד מהסקלארים מ- R.

6) חוג של פולינומים באינסוף משתנים

$$R[x_1,x_2,\dots]=\left\{\sum_{(i_1,i_2,\dots)=\bar{i}} a_{\bar{i}}\prod_{j=1}^{\infty}x_j^{i_j} \;\middle|\; a_{\bar{i}}\in R,\ \begin{array}{l}\text{עבור מספר סופי}\\ \text{של } \bar{i}\text{-ים}\end{array} a_{\bar{i}}\neq 0,\ (i_1,i_2,\dots)\in\mathbb{N}_0^{\mathbb{N}}\right\}$$

x_i, x_j מתחלפים כמו עם כל ואחד מהסקלארים

7) R תחום, נגדיר תחום של טורי חזקות

$$R[[x]] = \left\{ \sum_{k=0}^{\infty} a_k x^k \mid a_k \in R \right\}$$

חיבור:

$$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (a_k + b_k) x^k$$

כפל:

$$\left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j}\right) x^k$$

דוגמה:

$$(1+2x+3x^2+\dots)(2+4x-5x^2+\dots) = 2+(4x+2x\cdot 2)+(3x^2\cdot 2+2x\cdot 4x+1\cdot(-5x^2))+O(x^3) =$$

$$= 2+8x+9x^2+\dots$$

8) R תח"ש נגדיר תחום של פולינומים עם מספר סופי של משתנים

$$R\langle x_1,\dots,x_n\rangle = \left\{ \sum_{\bar{i}\in\mathbb{N}_0^n} a_{\bar{i}} x_1^{i_1}\cdots x_n^{i_n} \right\}$$

כאשר המשתנים x_i, x_j לא מתחלפים

דוגמה: $R\langle x_1, x_2\rangle$

$$(a_1x_1+a_2x_2)(b_1x_1+b_2x_2) = a_1b_1x_1^2 + a_1b_1x_1x_2 + a_2b_1x_2x_1 + a_2b_2x_2^2$$

9) תהי $M_n(R)$ מטריצות. כך R תחום

$$M_n(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} : a_{ij} \in R \right\}$$

חיבור וכפל של מטריצות

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ \cdots & \cdots \end{pmatrix}$$

$$0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \qquad 1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

וגילו גם R תחום, $M_n(R)$ לא תחום שכן בדוח

10) חוג של חבורה. יהי R חוג, G חבורה סופית.

$$R[G] = \{\sum_{g\in G} a_g \cdot g \mid a_g \in R\}$$

כפל:

$$(\sum_{g\in G} a_g \cdot g)(\sum_{h\in G} b_h \cdot h) = \sum_{(g,h)\in G} a_g b_h \cdot gh = \sum_{g\in G} g \cdot (\sum_{g\in G} a_{g^{-1}h} b_{g^{-1}}) = \sum_{g\in G} g \cdot (\sum_{g\in G} a_{hg^{-1}} b_g)$$

מיגור וכפל ב R

$$1 \cdot e = 1 \qquad 0 \cdot g = \sum_{g\in G} 0 = 0$$

11) הגאוסיים של גאוס

$$\mathbb{Z}[i] = \{a+bi : a,b\in\mathbb{Z}\} \subseteq \mathbb{C}$$

מיבור וכפל של מרוכבים

$$(a_1+b_1i)+(a_2+b_2i) = (a_1+a_2)+(b_1+b_2)i \in \mathbb{Z}[i]$$

$$(a_1+b_1i)(a_2+b_2i) = (a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i \in \mathbb{Z}[i]$$

הגדרה: יהי R חוג. תת קבוצה $S\subseteq R$ נקראת תת חוג אם S סגורה לחיבור ולכפל, $1\in S$, ו-S הוא חוג תחת הפעולות הנ"ל

טענה:

יהי R חוג, $S\subseteq R$ תת קבוצה. אז S תת-חוג אם ורק אם הוא מקיים את התנאים הבאים:

א) $1\in S$

ב) סגירות לחיסור: לכל $a,b\in S$ גם $a-b\in S$

ג) סגירות לכפל: לכל $a,b\in S$ גם $ab\in S$

ד) סגירות לחיבור: לכל $a,b\in S$ גם $a+b\in S$

סגור-ב, כ', מקומי

דוגמה?

$\mathbb{Z}[i]=S$ הינו תת-תוף של $\mathbb{R}=\mathbb{F}$

הוכחה?

(א', ב') כבר הוכחנו

(ג) $(a+bi)-(c+di)=(a-c)+(b-d)i\in\mathbb{Z}[i]$

(ד) $1=1+0i\in\mathbb{Z}[i]$

$\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}: a,b\in\mathbb{Z}\}\subseteq\mathbb{F}$

$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$

בקלות סגירות לכפל. שלושת התנאים האחרים ברורים. לכן $\mathbb{Z}[\sqrt{2}]$ הינו תת תוף של $\mathbb{F}$ (וגם $\mathbb{R}$)

$\mathbb{Z}[\sqrt{-5}]: \quad 6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$

בתרגיל לדוגמאות?

12) יהי $\alpha\in\mathbb{F}$ מספר מרוכב שהוא שורש של פולינום מתוקן עם מקדמים שלמים

α שורש של: $x^n+b_{n-1}x^{n-1}+\dots+b_1x+b_0$ $(b_i\in\mathbb{Z})$ (α נקרא שלם מעל $\mathbb{Z}$)

$\mathbb{Z}[\alpha]=\{c_0+c_1\alpha+\dots+c_{n-1}\alpha^{n-1} \mid c_1,\dots,c_{n-1}\in\mathbb{Z}\}$

סגירות לכפל: (נראה עבור α^k לכל $k\in\mathbb{N}$) כרוך $k\le n-1$

$k=n$ $\alpha^n+b_{n-1}\alpha^{n-1}+\dots+b_0=0$

$\alpha^n=-b_0-b_1\alpha-\dots-b_{n-1}\alpha^{n-1}\in\mathbb{Z}[\alpha]$

באינדוקציה ניתן $\alpha^k\in\mathbb{Z}[\alpha]$. לכן יומר

$\alpha^k=c_0+c_1\alpha+\dots+c_{n-1}\alpha^{n-1}$, $c_i\in\mathbb{Z}$

$$\alpha^{k+1} = \underbrace{c_0\alpha + c_1\alpha^2 + \dots + c_{n-2}\alpha^{n-1}}_{\in \mathbb{Z}[\alpha]} + \underbrace{c_{n-1}\alpha^n}_{\in \mathbb{Z}[\alpha]} \in \mathbb{Z}[\alpha]$$

$\bar{\mathbb{Z}} = \{\alpha \in \mathbb{C} \mid$ כלומר $\mathbb{Z}$ אפס מעל α ? α הינו שורש של פולינום מתוקן עם מקדמים שלמים$\}$

(13)

יהי α שורש המכורה של

$\sqrt[5]{12} \in \bar{\mathbb{Z}}$ $\quad x^5 - 12$

$\sqrt[7]{613} \in \bar{\mathbb{Z}}$ $\quad x^7 - 613$